

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-319329

(P2001-319329A)

(43) 公開日 平成13年11月16日 (2001.11.16)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード <sup>*</sup> (参考)
G 1 1 B 7/004		G 1 1 B 7/004	C 5 D 0 4 4
7/007		7/007	5 D 0 6 6
19/02	5 0 1	19/02	5 0 1 J 5 D 0 9 0
20/10		20/10	H

審査請求 未請求 請求項の数 9 O L (全 18 頁)

(21) 出願番号 特願2000-138392 (P2000-138392)

(22) 出願日 平成12年 5 月11日 (2000. 5. 11)

(71) 出願人 000204284

太陽誘電株式会社

東京都台東区上野 6 丁目16番20号

(72) 発明者 大村 幸秀

東京都台東区上野 6 丁目16番20号 太陽誘電株式会社内

(72) 発明者 砂川 隆一

東京都台東区上野 6 丁目16番20号 太陽誘電株式会社内

(74) 代理人 100096699

弁理士 鹿嶋 英資

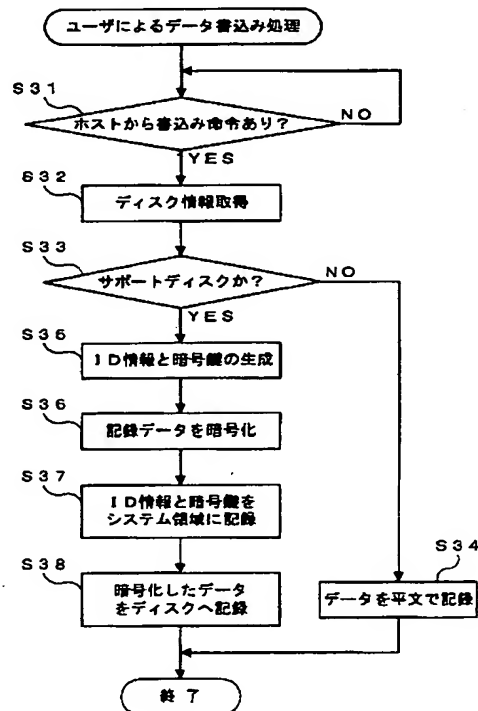
最終頁に続く

(54) 【発明の名称】 ライトワンス型光ディスク用記録装置および記録媒体

(57) 【要約】

【課題】 所定の製造者のライトワンス型光ディスクを使用した場合にのみ、そのライトワンス型光ディスクにセキュリティ性を持たせ、それ以外のライトワンス型光ディスクとの差別化を図る。

【解決手段】 ユーザデータを書き込むためのユーザ領域と少なくとも当該書き込み動作を行う際にシステムによって利用されるシステム領域とを備えたライトワンス型光ディスク用の記録装置において、前記ライトワンス型光ディスクの製造者を調べて所定の製造者（によって作られたライトワンス型光ディスク：図8においては「サポートディスク」）である場合に、前記システム領域の一部にセキュリティ対策のための情報を書き込む。所定の製造者によって作られたライトワンス型光ディスクについてのみ、そのシステム領域の一部にセキュリティ対策のための情報が書き込まれる。



**【特許請求の範囲】**

【請求項 1】 ユーザデータを書き込むためのユーザ領域と少なくとも当該書き込み動作を行う際にシステムによって利用されるシステム領域とを備えたライトワンス型光ディスク用の記録装置において、

前記ライトワンス型光ディスクの内部に電子的再生可能に記録された製造者情報を調べて所定の製造者情報である場合に、前記システム領域の一部にセキュリティ対策のための情報を書き込むようにしたことを特徴とするライトワンス型光ディスク用記録装置。

【請求項 2】 前記システム領域は、ユーザデータを書き込む際のレーザ強度キャリブレーション用領域であることを特徴とする請求項 1 記載のライトワンス型光ディスク用記録装置。

【請求項 3】 前記システム領域は、ユーザデータを書き込む際のセッション情報の一時格納用領域、または、ユーザ領域に書き込まれたユーザデータを再生する際に参照されるセッション情報格納用領域、若しくは、ユーザ領域の終了位置を明示するための領域のいずれかであることを特徴とする請求項 1 記載のライトワンス型光ディスク用記録装置。

【請求項 4】 前記セキュリティ対策のための情報は、前記ライトワンス型光ディスクの固体識別のための識別情報であることを特徴とする請求項 1 記載のライトワンス型光ディスク用記録装置。

【請求項 5】 前記セキュリティ対策のための情報は、ユーザ認証のための識別情報であることを特徴とする請求項 1 記載のライトワンス型光ディスク用記録装置。

【請求項 6】 前記セキュリティ対策のための情報は、前記ユーザデータを暗号化するための鍵情報であることを特徴とする請求項 1 記載のライトワンス型光ディスク用記録装置。

【請求項 7】 前記セキュリティ対策のための情報は、前記ユーザ領域に書き込まれた暗号化データを復号するための鍵情報であることを特徴とする請求項 1 記載のライトワンス型光ディスク用記録装置。

【請求項 8】 ライトワンス型光ディスクにアクセスするアクセス手段と、

前記アクセス手段を介して前記ライトワンス型光ディスクから製造者情報を読み出す読み出し手段と、

前記アクセス手段によって読み出された製造者情報が所定の製造者情報であるか否かを判定する判定手段と、

前記判定手段の判定結果が否でない場合に前記ライトワンス型光ディスクのシステム領域にセキュリティ対策のための情報を書き込む書き込み手段と、

を備えたことを特徴とするライトワンス型光ディスク用記録装置。

【請求項 9】 ライトワンス型光ディスクにアクセスするアクセス手段と、前記アクセス手段を介して前記ライトワンス型光ディスクから製造者情報を読み出す読み出

し手段と、

前記アクセス手段によって読み出された製造者情報が所定の製造者情報であるか否かを判定する判定手段と、前記判定手段の判定結果が否でない場合に前記ライトワンス型光ディスクのシステム領域にセキュリティ対策のための情報を書き込む書き込み手段とを実現するためのプログラムを格納したことを特徴とする記録媒体。

**【発明の詳細な説明】****【0001】**

【発明の属する技術分野】 本発明は、ライトワンス型光ディスク用記録装置および記録媒体に関する。詳しくは、1 回だけデータを書き込むことができる CD-R (Compact Disc Recordable) に代表されるライトワンス型光ディスクに適用する記録装置および記録媒体に関する。

**【0002】**

【従来の技術】 各種コンテンツやコンピュータプログラム等の電子データの配布媒体として、CD-ROM (Compact Disc Read Only Memory) が多用されている。CD-ROM は、電子データを記録したマスタ CD からプレス成型等によって製造される複製物であり、主に大量配布のメディアに用いられるが、配布数（製造数）の少ないサンプル版 CD やプライベート CD などには、ライトワンス型の光ディスク装置、典型的には CD-R が用いられる。CD-R は透明なディスク基板と反射層（詳細な構造は後述する。）との間に有機色素からなる記録層を有している点で CD-ROM と構造上の相違があり、専用の記録装置（CD-R ライター）を用いて当該記録層に高出力レーザを照射し、熱的反応によって当該記録層に情報ビットを形成することにより、ユーザ段階で情報の記録を行うことができるものである。

【0003】 CD-R は上記のとおり情報の消去や上書きができない（追記は可能）ライトワンス型である。すなわち、一度書き込んだ情報の消去や書き換えが不可能である。したがって、不正者による情報の消去や改ざんを確実に防止できるという優れた利点を持つことから、特に保全を要する電子データの保管や配布などの用途に欠かせない記憶媒体となっている。

**【0004】**

【発明が解決しようとする課題】 (1) しかしながら、従来のライトワンス型光ディスクにあっては、記録情報の消去や改ざんを防止できるという優れた利点があるものの、記録情報の読み出しが自由であるため、記録情報の不正読み出しや不正コピーを防止できないという不都合があった。このため、秘匿を要する情報を記録した CD-R の保管に際しては、厳格な管理規則を適用しなければならないが、このような管理規則の運用は相当困難で、多くの場合、規則の不徹底や馴れなどから安易な傾向に流れやすく、不心得な者による CD-R の持ち出しや情報の読み出しを阻止できない結果、秘匿すべき

情報の外部流出ないしは不正にコピーされたCD-Rの出現を回避できないという問題点があった。なお、かかる問題点は、CD-Rに限らず、可搬型の記憶デバイス一般にいえることであるが、CD-Rについては特に深刻である。CD-Rは、そのライトワンス型の特徴を活かして保全を要する電子データの配布や保管などに広く用いられている現実に加え、不要になったCD-Rを物理的に破壊（例えば、意図的に傷をつけたり切断したりする）しない限り、用済み後もその記録情報の不正読み取りが可能であるからである。

【0005】(2) また、従来のライトワンス型光ディスク、例えば、CD-Rにあつては、記録層に高出力レーザを照射し、熱的反応による情報ピットを形成することによって、ユーザ段階で情報の記録を行うものであるが、まれに、情報ピットの形成に失敗（書き込み失敗）したり、あるいは、情報ピットを形成できたとしてもその形成が不十分で読み出しの際にエラーを発生したり（読み出し失敗）することがある。こうしたトラブルは、特にノーブランド品を用いた場合に経験することがある。一般にノーブランド品の製造者責任は不明確であり、正規品（製造者を明示したもの）に比べて品質の悪いCD-Rの存在を否定できないからである。このような背景を考慮すると、理想的にはユーザに対して正規品の使用を推奨すべきであるが、実際にはノーブランド品は正規品に比べて安価に入手できることなどの理由から、ノーブランド品の利用者は結構多く、一部とはいえ粗悪品の存在に起因する上記トラブルの発生が問題となっている。

【0006】したがって、本発明が解決しようとする課題は、所定の製造者のライトワンス型光ディスクを使用した場合にのみ、そのライトワンス型光ディスクにセキュリティ性を持たせることができ、以って、それ以外のライトワンス型光ディスクとの差別化を図ることにある。

#### 【0007】

【課題を解決するための手段】請求項1記載のライトワンス型光ディスク用記録装置は、ユーザデータを書き込むためのユーザ領域と少なくとも当該書き込み動作を行う際にシステムによって利用されるシステム領域とを備えたライトワンス型光ディスク用の記録装置において、前記ライトワンス型光ディスクの内部に電子的再生可能に記録された製造者情報を調べて所定の製造者情報である場合に、前記システム領域の一部にセキュリティ対策のための情報を書き込むようにしたことを特徴とする。これによれば、所定の製造者によって作られたライトワンス型光ディスクについてのみ、そのシステム領域の一部にセキュリティ対策のための情報が書き込まれる。

【0008】請求項2記載のライトワンス型光ディスク用記録装置は、請求項1記載のライトワンス型光ディスク用記録装置において、前記システム領域は、ユーザデ

ータを書き込む際のレーザ強度キャリブレーション用領域であることを特徴とする。これによれば、データの再生時にその存在が無視される特定の領域（レーザ強度キャリブレーション用領域）にセキュリティ対策のための情報が書き込まれる。

【0009】請求項3記載のライトワンス型光ディスク用記録装置は、請求項1記載のライトワンス型光ディスク用記録装置において、前記システム領域は、ユーザデータを書き込む際のセッション情報の一時格納用領域、または、ユーザ領域に書き込まれたユーザデータを再生する際に参照されるセッション情報格納用領域、若しくは、ユーザ領域の終了位置を明示するための領域のいずれかであることを特徴とする。これによれば、いずれもユーザからの直接的なアクセスが許容されていない領域にセキュリティ対策のための情報が書き込まれる。

【0010】請求項4記載のライトワンス型光ディスク用記録装置は、請求項1記載のライトワンス型光ディスク用記録装置において、前記セキュリティ対策のための情報は、前記ライトワンス型光ディスクの固体識別のための識別情報であることを特徴とする。これによれば、ライトワンス型光ディスクの固体識別に基づくセキュリティ対策が可能となる。

【0011】請求項5記載のライトワンス型光ディスク用記録装置は、請求項1記載のライトワンス型光ディスク用記録装置において、前記セキュリティ対策のための情報は、ユーザ認証のための識別情報であることを特徴とする。これによれば、セキュリティ対策のための情報を利用したユーザ認証が可能となる。

【0012】請求項6記載のライトワンス型光ディスク用記録装置は、請求項1記載のライトワンス型光ディスク用記録装置において、前記セキュリティ対策のための情報は、前記ユーザデータを暗号化するための鍵情報であることを特徴とする。これによれば、セキュリティ対策のための情報を利用したユーザデータの暗号化が可能となる。

【0013】請求項7記載のライトワンス型光ディスク用記録装置は、請求項1記載のライトワンス型光ディスク用記録装置において、前記セキュリティ対策のための情報は、前記ユーザ領域に書き込まれた暗号化データを復号するための鍵情報であることを特徴とする。これによれば、セキュリティ対策のための情報を利用した暗号化データの復号が可能となる。

【0014】請求項8記載のライトワンス型光ディスク用記録装置は、ライトワンス型光ディスクにアクセスするアクセス手段と、前記アクセス手段を介して前記ライトワンス型光ディスクから製造者情報を読み出す読み出し手段と、前記アクセス手段によって読み出された製造者情報が所定の製造者情報であるか否かを判定する判定手段と、前記判定手段の判定結果が否でない場合に前記ライトワンス型光ディスクのシステム領域にセキュリテ

ィ対策のための情報を書き込む書き込み手段と、を備えたことを特徴とする。これによれば、所定の製造者によって作られたライトワンス型光ディスクについてのみ、そのシステム領域にセキュリティ対策のための情報が書き込まれる。

【0015】請求項9記載の記録媒体は、ライトワンス型光ディスクにアクセスするアクセス手段と、前記アクセス手段を介して前記ライトワンス型光ディスクから製造者情報を読み出す読み出し手段と、前記アクセス手段によって読み出された製造者情報が所定の製造者情報であるか否かを判定する判定手段と、前記判定手段の判定結果が否でない場合に前記ライトワンス型光ディスクのシステム領域にセキュリティ対策のための情報を書き込む書き込み手段とを実現するためのプログラムを格納したことを特徴とする。これによれば、マイクロコンピュータを含むハードウェア資産と該プログラムとの有機的結合によって前記アクセス手段、読み出し手段、判定手段および書き込み手段が実現される。

#### 【0016】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を詳細に説明する。なお、以下の説明における様々な細部の特定ないし実例および数値や文字列その他の記号の例示は、本発明の思想を明瞭にするための、あくまでも参考であって、それらのすべてまたは一部によって本発明の思想が限定されないことは明らかである。また、周知の手法、周知の手順、周知のアーキテクチャおよび周知の回路構成等（以下「周知事項」）についてはその細部にわたる説明を避けるが、これも説明を簡潔にするためであって、これら周知事項のすべてまたは一部を意図的に排除するものではない。かかる周知事項は本発明の出願時点で当業者の知り得るところであるので、以下の説明に当然含まれている。

【0017】図1は、ライトワンス型光ディスク（以下「CD-R」という。）の外観図（a）およびその要部拡大図（b）である。これらの図において、CD-R1は、直径12cm（直径8cmのものもある。以下、直径12cmのもので説明する。）のディスク状を有しており、ディスクの中心に直径15mmのセンターホール1aが形成されている。ディスクの中心T0からセンターホール1aの壁（ディスク内縁T1）までの距離は7.5mm、T0からディスク外縁T7までの距離は60mmであり、このT1～T7の間に同心状の複数の記録領域、すなわち、ディスクの内周側から順にPCA（Power Calibration Area）、PMA（Program Memory Area）、リードイン（図では「RI」と略している。）、データエリア（図では「UA」と略している。）およびリードアウト（図では「RO」と略している。）の各領域が設けられている。

【0018】各領域を概説すると、T2～T3に位置するPCAは、CD-R1にデータを記録する際に行われ

るレーザ強度調整のための試し書き領域である。この試し書きは一般に100回程度可能であり、少なくとも1回のデータ記録で1回分の領域を消費する。T3～T4に位置するPMAは、CD-R1でまだクローズしていないセッションのトラックがあるとき、そのトラック番号と開始／終了位置を一時的に保存する領域である。T4～T5に位置するリードイン（RI）は、セッショントラックの先頭（ディスクの内周側）にある領域で、セッションのTOC（Table Of Contents：CDに記録されているトラック数、開始位置およびデータ領域の合計の長さ）を保存する領域である。セッションをクローズすると、PMAに一時保存されていた情報がこのリードイン（RI）に書き込まれる。

【0019】T5～T6に位置するデータエリア（UA）は、ユーザ段階で実際にデータが書き込まれる領域である。データの記録容量は最大約680Mバイト（直径8cmのものは最大約190Mバイト）であり、この記憶容量は録音時間で表すと最大約74分（直径8cmのものは最大約21分）になる。データエリア（UA）は、リードイン（RI）のすぐ後ろから連続する所定サイズ（2Kバイト）単位の論理ブロックで管理されるようになっており、各論理ブロックごとに0から最大約330000までのLBN（Logical Block Number）が割り当てられるようになっている。T6～T7に位置するリードアウト（RO）は、セッションの最後（ディスクの外周側）にある領域で、データエリア（UA）の最後に到達したことを示す領域である。

【0020】これら各領域のディスク上の位置はT3を除いて規格化されている。すなわち、T2はT0から2.5mm離れた位置、T4はT0から23mm離れた位置、T5はT0から25mm離れた位置、T6はT0から58mm離れた位置となるように規定されている。なお、図ではディスク外縁とリードアウト（RO）の終了位置とを同一の符号（T7）で示しているが、これは図示の都合である。リードアウト（RO）の実際の終了位置はT0から58.5mm離れた位置になる。以下、特に断りのない限り、T7はリードアウト（RO）の終了位置を表すものとする。ちなみに、リードアウト（RO）の開始と終了位置（T6およびT7）はCD-R1に記録するデータの量に応じて変化する。上記の実際値（T6＝58mm、T7＝58.5mm）は記憶データ量を最大にしたときのものである。

【0021】図2は、CD-R1の断面構造図である。CD-R1は、透明で耐熱性、耐湿性および成形性に優れ、且つ、所要の光学的特性（屈折率や複屈折など）を備えた材料（例えばプラスチック）からなる基板1bの上に、有機色素からなる記録層1c、アルミニウムなどの金属材料からなる反射層1dおよび樹脂等の硬質材料からなる保護層1eを積層して形成されている。断面全体の厚さは1.2mmである。

【0022】CD-ROMとの構造上の相違は、記録層1cを有する点、および記録層1cと基板1bとの間にウォブルグループと呼ばれる渦巻状の案内溝1fが形成されている点にある。CD-R1へのデータの記録は基板1bの裏側から案内溝1fに沿って記録用の強いレーザを照射し、記録層1cを加熱して情報ピット(pit:再生用のレーザ反射光を変調するための物理的変形変質部分)を形成することにより行われる。

【0023】図3は、CD-R1の案内溝1f(ウォブルグループ)を示す模式図である。案内溝1fは同図(a)に示すように、ディスクの内周側から外周側(または外周側から内周側)に向かって一筆書きの要領で連続して形成されており、案内溝1fの幅は約0.5~0.7μm、間隔は約1.6μmである。ユーザ段階におけるデータ記録は、案内溝1fに沿って、その案内溝1f(または案内溝1fの間のランド部)直下の記録層1cに情報ピットを形成することによって行われる。なお、CD-R1の裏側から見て案内溝1fの凸部分をランド(山)、凹部分をグループ(谷)といい、一般に谷の部分ウォブルグループというが、本明細書では山と谷を区別しない。

【0024】ここで、案内溝1fの一の役割は、ユーザ段階のデータ記録時にディスクの回転速度を制御するためのタイミング情報を保持することにある。この役割のため、案内溝1fは、同図(b)に示すように、所定の周期T1(例えばT1は22.05kHzに相当する周期)で蛇行(「ウォブリング」ともいう。)する形状に形成されている。データの記録時には、この蛇行を光ピックアップでトレースして周期T1を検出し、その検出周期T1が一定となるようにディスクの回転速度を制御することにより、データ記録時の光ピックアップとディスク間の相対速度を一定に保つ。

【0025】案内溝1fの他の役割は、ディスク上の各記録領域(PCA、PMA、RI、UAおよびRO)の位置情報をはじめとした様々なディスク情報を保持することにある。ディスク情報はATIP(Absolute Time In Pregroove:通称「Aチップ」という。)とも呼ばれており、ATIPには、上記の位置情報のほかに、基準の記録レーザ強度やディスク回転速度、アプリケーションコードあるいはディスクタイプなどの各種情報が含まれると共に、さらに、ディスクの製造者を特定可能な情報(以下「製造者情報」という。)も含まれる。例えば、リードイン(RI)の開始位置情報はディスクの製造者ごとに異なるため、この開始位置情報を製造者情報として利用することができる。

【0026】実際の案内溝1fは、例えば、同図(c)に示すように、さらに細かく蛇行(または変形)しており、その細蛇行の周期T2によってATIP情報を多重化している。データの記録時にその周期(周波数)差を利用してタイミング情報とATIP情報を分離抽出し、

タイミング情報を用いてディスクの回転制御を行うと共に、ATIP情報を用いてデータ記録位置等の制御を行うことが可能となる。

【0027】なお、図示の例では、案内溝1fの細蛇行周期T2によってATIP情報の多重化を行っているが、この態様に限定されない。要は、データの記録時に案内溝1fをトレースしてそのトレース信号からATIP情報を再生できればよく、例えば、案内溝1fの側壁に凹凸等の物理的特異変形部分を形成し、その特異変形部分の間隔等からATIP情報を再生することも可能である。以下、説明の都合上、ATIP情報は上記の細蛇行周期T2によって多重化されているものとする。

【0028】図4は、CD-R1に案内溝1fを形成するために、主としてディスクの製造段階で用いられる製造装置10の構成図である。この図において、製造装置10は、周期T1のタイミング情報に基づいて同期信号用ウォブリング信号(以下「同期ウォブル信号」という。)を発生する第1ウォブリング信号発生回路11と、少なくともディスクの製造者情報を含むATIP信号に基づいてATIPウォブル信号を発生する第2ウォブリング信号発生回路12と、第1アンプ13を介して同期ウォブル信号を取り込み、この同期ウォブル信号を用いて、不図示のレーザ光源から発射されたレーザ光を変調する第1光変調器15と、第2アンプ14を介してATIPウォブル信号を取り込み、このATIPウォブル信号を用いて、第1光変調器15を通過したレーザ光を変調する第2光変調器16と、第2光変調器16を通過したレーザ光を反射するミラー17と、ミラー17で反射されたレーザ光を絞り込んでCD-R1の記録面に照射する対物レンズ18と、CD-R1を回転駆動するモータ19とを備え、上記レーザ光の記録面への照射位置をCD-R1の半径方向に移動させつつ、当該CD-R1を回転駆動することにより、図3(a)に示す渦巻状の案内溝1fを形成する。

【0029】ここで、第1光変調器15を通過したレーザ光は同期ウォブル信号による変調を受けており、さらに第2光変調器16を通過したレーザ光はATIPウォブル信号による変調を受けている。すなわち、レーザ光は都合2回、変調されることとなる。したがって、CD-R1の記録面に形成される案内溝1fは、同期ウォブル信号の周期T1とATIPウォブル信号の周期T2との合成周期に対応して「ウォブリング」(蛇行)することとなり、結局、図3(c)に示すように、二つの周期(T1、T2)を有する合成蛇行形状が得られる。

【0030】図5は、CD-R1の各記録領域のフォーマット概念図である。この図において、PCA、PMA、リードイン(RI)、データエリア(UA)およびリードアウト(RO)はそれぞれ、図1(b)における同名部分に対応する。PCAおよびPMAのサイズ(情

報書き込み可能容量)は特に決められていないが、前述の試し書き回数(一般に100回程度)やセッション情報の一時記憶回数に見合った必要量、例えば、PCAで約3.5Mバイト程度、PMAで約2Mバイト程度の容量が確保されている。ちなみに、これらの例示容量からPCAの開始位置(T2)とPMAの開始位置(T3)は、規格化されたリードイン(RI)の開始位置(T4)を基準として、「 $T2 = T4 - \text{約} 3.5 \text{ 秒}$ 」の位置、「 $T3 = T4 - \text{約} 1.3 \text{ 秒}$ 」の位置と書き表すことができる。

【0031】既述のとおり、PCAはデータ記録を行う際の試し書き領域、PMAはクローズされていないセッション情報を一時的に格納する領域であるから、これら二つの領域(PCA/PMA)はデータ記録時のみ利用(アクセス)される領域である。一方、リードイン(RI)はクローズされたセッション情報をTOCとして記録する領域、データエリア(UA)は実際にデータが書き込まれる領域、リードアウト(RO)はデータエリアの終わりを明示する領域であるから、これら三つの領域(リードイン/データエリア/リードアウト)はデータ記録時と再生時の両方で利用(アクセス)される領域である。

【0032】他方、これらすべての領域をユーザからのアクセス容易性の点で見ると、すなわち、CD-R1の読み取り装置を備えたパーソナルコンピュータ等の利用者からその記憶内容を通常のツール(典型的には当該パーソナルコンピュータに搭載されたオペレーティングシステム上のファイルシステムなど)を用いて容易にアクセスできるか否かの点で評価すると、データエリア(UA)については当然ながらその記憶内容の全容把握は可能であるが、他の領域(PCA、PMA、リードインおよびリードアウト)の内容把握は不可能である。

【0033】もちろん、特殊なツールを使用すれば可能ではあるが、そのようなツールは一般のユーザにとって入手困難であるため、かかる例外的なツールの利用を除けば、データエリア以外の他の領域(PCA、PMA、リードインおよびリードアウト)は、システムからのアクセスだけが許可された特殊な領域であるといえる。以下、この特殊領域のことを「システム領域」といい、ユーザからのアクセスが許可された領域のことを「ユーザ領域」ということにする。すなわち、データエリア(UA)はユーザ領域、それ以外のPCA、PMA、リードイン(RI)およびリードアウト(RO)はシステム領域である。

【0034】さて、本実施の形態におけるCD-R1のポイントは、後述するように、①ユーザ段階でデータ記録を行う際にCD-R1の製造者(CD-R1に書き込まれている製造者情報)を調べ、その製造者(製造者情報)が所定のサポートリストに記載されている場合に、当該CD-R1のシステム領域の一部にCD-R1の固

体識別情報(以下「ID情報」という。)と、所定の暗号鍵情報とを書き込むようにした点にある。②また、データ記録時に暗号鍵を用いて記録データを暗号化し、当該暗号化データを当該CD-R1に書き込むようにした点にある。③さらに、暗号化データを記録したCD-R1のデータ再生やディスクコピーを行う際に、前記ID情報に基づくユーザ認証を行うようにした点にある。

【0035】これらの①～③のポイントによって、秘匿を要するデータの管理や配布にセキュリティ性を持たせることができるようになる。すなわち、データを暗号化してCD-R1に記録できる(②)とともに、この暗号化データを再生(復号)する際に、ID情報によるユーザ認証を行い(③)、正規ユーザ(ID情報を知っているユーザ)に対してのみデータ再生を許可することができるようになる。

【0036】かかるセキュリティ機能は、CD-R1に最初から付加されているものではなく、ある条件を満たした場合に付加される機能である。すなわち、CD-R1の製造者が所定のサポートリストに記載されている場合にのみ(①)付加される限定的な機能であり、言い換えれば、サポートリストに記載されていない製造者(または製造者不明)のCD-Rには付加されない機能であるから、この機能の有無によってCD-Rの差別化を図ることができる。

【0037】冒頭で説明したように、ユーザが市場で入手可能なCD-R1は、製造者を明示した正規品とそれ以外の非正規品(ノーブランド品)とに分けられる。ノーブランド品は低価格であるものの粗悪品の存在を否定できないため、まれではあるが正常なデータ記録を行えないことがあった。特に重要なデータの管理や配布用途には正規品の使用を強制すべきであるが、そのような強制は実際上困難であるから、ノーブランド品の使用に伴うデータ書き込み失敗や読み出し失敗等のトラブルの可能性を認めなかった。

【0038】本実施の形態におけるCD-R1は、ユーザリストに記載された製造者のCD-R1を使用することにより、ユーザは上記のセキュリティ機能を利用できるようになる。換言すれば、ユーザリストに記載されていないノーブランド品を使用した場合は上記のセキュリティ機能を利用できないから、特に秘匿を要するデータの保管や配布に適用する場合、ユーザは正規品を使用せざるを得なくなり、結果的にノーブランド品の使用を排除して、粗悪品に起因する記録データの書き込み失敗や読み出し失敗といったトラブルを回避することができるという格別のメリットが得られる。

【0039】CD-R1のシステム領域に書き込むID情報はCD-R1の全製造数にわたってユニークな値(重複しない値)を持つことが望ましいが、製造数が膨大になる場合、情報ビットが多ビット化してシステム領域の記憶容量を圧迫する懸念があるため、例えば、製造

ロットごとや製造ラインごとまたは製造時期ごとに異なる情報としてもよい。このID情報は、後述するように、データ再生やデータコピーを行う際のCD-R1へのアクセス照合に用いられる。データの再生等を行うアプリケーションでIDの入力を要求し、入力されたIDとシステム領域に書き込まれているIDとの一致を判定して、一致の場合のみアクセスを許可する。これにより、不正なユーザ（IDを知らないユーザ）によるデータの再生や複製を阻止し、データの流出や不正生成物の出現を回避することができる。

【0040】ID情報の入手方法は、次の二つのものが考えられる。第一の方法はID情報を印刷した紙片をCD-R1のパッケージに入れて一緒に出荷するというものである。ユーザはその紙片を見ながらID情報を入力する。この方法はパッケージソフトの分野で一般的に行われているインストール登録方法と類似しており、紙片を紛失しない限り、最も確実に簡単な方法である。なお、この方法の変形として、パッケージの表面やラベルにID情報を印刷したりすることもあるが、いずれもCD-R1と一緒に適切なID情報をユーザに届けるという点で同一である。第二の方法はインターネット上の所定のWebサイトからID情報を入手するというものである。このWebサイトはあらゆるメーカ製のCD-RについてユニークなID情報を発行できるように構成された動的Webサイトであり、ユーザからのID情報発行要求に回答して適切なID情報を当該ユーザ宛てに交付することができるものである。このようなWebサイトは、例えば、WWWサーバ上で動作するASP（Active Server Pages）やCGI（Common Gateway Interface）等のサーバサイドスクリプトエンジンとデータベースとの組み合わせで構築することができる。この場合、CD-Rのパッケージには事前に登録用のコード情報（メーカ別またはその他の識別情報を示すコード情報）を印刷した紙片を入れておくことが望ましい。ユーザはこのコード情報を用いてID情報の交付を要求する。Webサイトは入力されたコード情報と交付済みID情報とをデータベースに登録して管理する。さらに第二の方法は次のように発展させることもできる。ユーザは初回のID情報発行要求時にそのユーザ専用のユーザ識別情報をWebサイトから受け取り、当該ユーザは以降のID情報発行要求時にそのユーザ識別情報を用いてWebサイトにアクセスする。このようにすると、Webサイトは交付済みID情報の履歴管理をユーザ識別情報ごと（すなわち、各ユーザごと）に行うことが可能となり、ユーザは過去に使用したID情報の履歴情報をWebサイトにアクセスしていつでも見ることができる。したがって、ユーザにとっては、自分で履歴管理をしなくてもよいというメリットが得られる。

【0041】一方、システム領域と一緒に書き込まれる鍵情報に、ユーザ段階でデータエリアに書き込まれる生

データを暗号化するために用いられる。すなわち、データの記録を行うアプリケーションで暗号鍵を読み出し、この暗号鍵を用いて生データを暗号化データに変換した後、その暗号化データをCD-R1のデータエリアに書き込む。この暗号鍵は暗号化データを復号する際にも用いられる。すなわち、データの再生時に、データの再生を行うアプリケーションでIDの入力を要求し、入力されたIDとシステム領域に書き込まれているIDとの一致を判定して、一致の場合に暗号鍵と暗号化データを読み出し、その暗号鍵を用いて暗号化データを復号し、生データに変換してユーザの利用に供する。

【0042】したがって、IDを知らない不正なユーザは、データへのアクセス自体を拒否されるから、不正なデータの読み取りを回避できると共に、万が一、何らかの手段でアクセスが成功したとしても、システム領域に書き込まれた暗号鍵へのアクセスは通常の技術知識では不可能であるから、暗号化データを生データに復号することができず、この点において万全の保全策を講じることができる。

【0043】図6は、システム領域に書き込まれるID情報と暗号鍵を含むデータフォーマットの例示構造図である。この図において、第一の例（a）は、8バイトのID情報、8バイトのDES（Data Encryption Standard：アメリカ連邦政府標準暗号規格）暗号鍵、2バイトの製造年、1バイトの製造月および1バイトの製造日の各情報から構成された全部で20バイトの大きさを有している。また、第二の例（b）は、8バイトのID情報、24バイトのトリプルDES暗号鍵、2バイトの製造年、1バイトの製造月および1バイトの製造日の各情報から構成された全部で36バイトの大きさを有している。

【0044】いずれのフォーマットを採用するかは、もっぱら暗号鍵の信頼性を重視するか、または、システム領域の記憶容量圧迫を回避するかで決まる。なお、図示のバイト数や暗号鍵の種類およびフォーマット構造はあくまでも例示である。要はCD-R1の固体識別が可能で情報（ID情報）と、生データを暗号化データに変換できると共に暗号化データから生データに復号できる所定のキー情報（暗号鍵）とをCD-R1のシステム領域に書き込んでおけばよい。

【0045】図7は、ライトワンス型光ディスク記録再生装置（以下「CD-R記録再生装置」という。）の概略的なブロック構成図である。このCD-R記録再生装置30は、CD-R1のクランピングエリア（図1

（a）のT1～T2の間に設けられた情報非記録エリア）を担持して所定方向に回転駆動するスピンドルモータ31と、CD-R1の基板1bを透過して記録層1cに記録用または再生用のレーザ（一般に波長770～830nmの赤外レーザ）32を照射する光ピックアップ33と、光ピックアップ33の内部に設けられた不図示の



シークモータと協調して光ピックアップ33をディスクの半径方向に移動させる粗動モータ34とを備えると共に、スピンドルモータ31の回転速度を制御するディスク回転制御部35と、粗動モータ34の回転速度と回転方向を制御する粗動モータ制御部36と、光ピックアップ33の位置やレーザ強度の制御を行うピックアップ制御部37と、CD-R1の案内溝1fのトレース信号から同期ウォッブル信号やATIPウォッブル信号を検出して、ディスク回転制御のためのタイミング情報や少なくともディスクの製造者を特定可能な情報を含むATIP情報を再生するウォブリング制御部38と、光ピックアップ33からの読み取り信号や光ピックアップ33への書き込み信号の波形変換等の制御を行う再生/記録制御部39とを備え、さらに、これらの各制御部を統括するコントローラ40を備える。このコントローラ40は、発明の要旨に記載のアクセス手段、読み出し手段、判定手段および書き込み手段に相当する。

【0046】CD-R記録再生装置30は、パーソナルコンピュータ等のホスト装置41の拡張スロットに内蔵され（または外付けされ）、ホスト装置41とコントローラ40との間を所定の信号規格（例えば、SCSI: Small Computer System Interface）のケーブル41aで接続して用いられる。

【0047】このような構成を有するCD-R記録再生装置30は、以下に示すとおり、CD-R1への情報の記録とその記録情報の再生を行うことができる。なお、CD-R1はCD-ROMコンパチのデバイスであり、CD-R記録再生装置30は、CD-ROMの情報再生も可能であるが、本発明とは直接の関連がないため説明を省略する。

【0048】<CD-R1への情報の記録動作>ホスト装置41でCD-R記録専用アプリケーションプログラム（以下「AP」と省略する。）を実行すると、まず、APからのレーザ強度キャリブレーションコマンドがコントローラ40に伝えられる。コントローラ40はこのコマンドに応じて各制御部に所要の指令を伝え、光ピックアップ33をCD-R1のPCA空領域（試し書きされていない領域）に位置させると共に、スピンドルモータ31の回転速度を制御（光ピックアップ33の現在位置における相対速度が所定速度となるように制御）した後、光ピックアップ33から暫定強度（5.5～8mWの間の任意パワー）の記録用レーザ32をPCA空領域に照射して試し書きを行う。光ピックアップ33の位置制御およびスピンドルモータ31の回転速度制御はCD-R1の案内溝1fのトレース信号から再生された情報（タイミング情報およびATIP情報）に従って行われる。

【0049】次いで、コントローラ40は、再生/記録制御部39を介してPCAに試し書きされたデータを読み取り、そのデータをホスト装置41のAPに返送す

る。APは、試し書きデータと期待値とを比較してレーザ強度の適否を判定し、判定結果が“否”であればレーザ強度を増減調節して再びレーザ強度キャリブレーションコマンドを発行する一方、判定結果が“適”であれば、CD-R1への情報の記録動作を開始する。

【0050】この記録動作は、ユーザによって適宜に選択された所要の記録データをAPからコントローラ40に伝え、このコントローラ40の制御の下、各制御部を介してスピンドルモータ31の回転制御および光ピックアップ33の位置制御を行いつつ、上記記録データで光ピックアップ33からの記録用レーザ32を変調しながらCD-R1のデータエリアに記録を行っていくというものである。そして、記録を完了すると、すべてのセッションを閉じ、そのセッション情報のTOCをリードイン（R1）に書き込むと共に、最終セッションの後にリードアウト（R0）を形成する。

【0051】<CD-R1の記録情報の再生動作>CD-R1の記録情報を再生する際に上記AP（CD-R記録専用アプリケーションプログラム）は不要である。但し、CD-R1のファイルシステムとホスト装置41のファイルシステムとの相互変換を行うためのドライバソフトは必須である。ユーザはこのドライバソフトを介してCD-R記録再生装置30を利用することにより、ホスト装置41に装備されたハードディスク等の他の記憶デバイスとの区別を意識せずにCD-R1のファイルシステムにアクセスすることができる。すなわち、ユーザにはオペレーティングシステムのファイルシステムによって認識されたファイル構造が見えるから、ユーザは、他の記憶デバイスに格納されたファイルと同様の手順でCD-R1内の目的とするファイルを選択し、そのファイルをコピーして他の記憶デバイスに貼り付けたり、またはEXE形式等の実行ファイルの場合は当該ファイルをオープンして実行したりすることができる。

【0052】CD-R記録再生装置30は、このファイルアクセスに際して、リードイン（R1）内のTOC情報を読み出してホスト装置41のドライバソフトに提供すると共に、当該ドライバソフトから特定ファイルの読み出しコマンドを受け取った場合は、リードイン（R1）内のTOC情報を参照して当該ファイルのデータが書き込まれたデータエリア（UA）のトラックを特定し、そのトラックの開始位置に光ピックアップ33を位置させると共に、スピンドルモータ31の回転速度を制御し、光ピックアップ33から再生用のレーザ（パワーが0.2mW程度に抑えられる点を除き記録用のレーザと同じもの）13をCD-R1に照射して当該ファイルデータを読み取り、その読み取りデータをホスト装置41に転送するという一連の動作を実行する。

【0053】以上のとおり、本実施の形態のCD-R記録再生装置30は、CD-R1への情報の書き込みを行うことができると共に、CD-R1に書き込まれた情報

10

20

30

40

50



の再生も行うことができる。このCD-R記録再生装置30は、ユーザ段階でCD-R1への情報の書き込みを行う場合に必要不可欠な構成要素であるが、ユーザ段階で、CD-R1に書き込まれた情報の再生を行う場合も必要とされる構成要素である。CD-R1はCD-ROMコンパチのデバイスで、昨今のパーソナルコンピュータ等のほとんどにはCD-ROM再生装置が搭載されており、そのCD-ROM再生装置を利用してCD-R1の情報再生を行うことも可能であるが、このCD-ROM再生装置は、CD-R1のシステム領域に書き込まれたID情報や暗号鍵にアクセスできないから、やはり、CD-R1に書き込まれた情報の再生を行う場合もCD-R記録再生装置30は欠かせない構成要素である。

【0054】<ユーザによるデータ書き込み処理>図8は、ユーザ段階で実行されるデータ書き込み動作（以下「ユーザによるデータ書き込み処理」という。）を示すフローチャートである。この処理では、ユーザは、データ未記録のCD-R1を市場で入手し、そのCD-R1をCD-R記録再生装置30にセットして、所要のユーザデータを当該CD-R1に記録する。このユーザデータについて、とりわけ重要な点は、特定の人に対してのみ再生を許可する非公開のデータ、すなわち、秘匿を要するデータである点にある。従来、この種の秘匿を要するデータをCD-Rに記録する場合は、例えば、所定の暗号鍵でデータを暗号化してCD-Rに記録し、そのCD-Rと一緒に当該暗号化データの復号鍵を収めたフロッピーディスク等の記憶媒体を配布していた。しかし、このような複数媒体の同時配布は手間がかかる上、配布先での紛失等の可能性もあり、管理が面倒であるという欠点がある。

【0055】本実施の形態のCD-R1は、一つの記憶媒体に暗号化データと、その暗号化データの復号鍵とを収めて配布するので、配布先で紛失することなく、管理を容易にして上記不都合を解消できるというメリットがある。

【0056】図8において、ユーザによるデータ書き込み処理を開始すると、CD-R記録再生装置30は、ホスト装置41からの書き込み命令の有無を判定する（ステップS31）。そして、書き込み命令があると、CD-R1のディスク情報を取得する（ステップS32）。このディスク情報は当該CD-R1の製造者を特定可能な情報であり、例えば、ATIP情報に含まれる、リードイン（R1）の開始位置情報である。この開始位置情報はディスクの製造者ごとに異なるため、この開始位置情報から製造者を割り出すことが可能であるからである。

【0057】ディスク情報を取得すると、次に、そのディスク情報と所定のサポートリストとを照合して、当該CD-R1の製造者がサポートリストに記載されているか否かを判定する（ステップS33）。サポートリスト

は、例えば、コントローラ40の内部に設けられた不揮発性メモリ（好ましくはリストの更新を可能にするためフラッシュメモリ等の書き換え可能な不揮発性メモリ）に記録されたものであり、当該CD-R1の製造者がサポートリストに記載されていない場合は、当該CD-R1は後述のセキュリティモードをサポートしないディスク（非サポートディスク）であるとして、ユーザデータを平文（暗号化されない生のデータ）で当該CD-R1のユーザエリア（UA）に記録（ステップS34）した後、処理を終了する。なお、上記サポートリストのダウンロードサービスを構築しておくことが望ましい。このような配布方式は、例えば、WWW（World Wide Web）サーバやFTP（File Transform Protocol）サーバ等のインターネット技術を用いることによって容易に実現することができる。

【0058】一方、当該CD-R1の製造者がサポートリストに記載されている場合は、当該CD-R1は後述のセキュリティモードをサポートするディスク（サポートディスク）であるとして、まず、ID情報と暗号鍵を生成する（ステップS35）。ID情報は、前述したように、例えば、ユーザの身元情報と引き換えに第三者機関から取得したものである。次に、その暗号鍵を用いてユーザデータを暗号化（ステップS36）した後、ID情報および暗号鍵ならびに記録日付等の情報を当該CD-R1のシステム領域に書き込み（ステップS37）、さらに、暗号化データを当該CD-R1のユーザエリア（UA）に書き込んで（ステップS38）処理を終了する。なお、ステップS37において、CD-R1のシステム領域に書き込むID情報や暗号鍵ならびに記録日付等の情報のフォーマットは、図4（a）または（b）に示すとおりである。

【0059】図9は、上記「ユーザによるデータ書き込み処理」のタイムランを示す図であり、図中のパーソナルコンピュータ51は上述のホスト装置41に相当するもの、CD-Rライター52は上述のCD-R記録再生装置30に相当するもの、CD-R53は上述のCD-R1に相当するものである。

【0060】この図において、ユーザは、CD-R53をCD-Rライター52に装填すると共に、パーソナルコンピュータ51を操作して所要の書き込み命令をCD-Rライター52に発行する。CD-Rライター52はこの書き込み命令に応答して、CD-R53のディスク情報を取得し、そのディスク情報に含まれる製造者情報と所定のサポートリストとを照合してサポートディスクであるか否かを判定する。そして、サポートディスクでなければ、パーソナルコンピュータ51にノーマルモードでの動作を通知し、パーソナルコンピュータ51はこの通知に応答してユーザデータを平文でCD-Rライター52に転送し、CD-Rライター52はパーソナルコンピュータ51から転送された平文のユーザデータをC

CD-R 53のユーザエリア(UA)に書き込む。

【0061】一方、ディスク情報に含まれる製造者情報と所定のサポートリストとを照合した結果、サポートディスクであることを判定した場合は、CD-Rライター52はパーソナルコンピュータ51に対してセキュリティモードでの動作を通知し、パーソナルコンピュータ51はこの通知に応答して、ID情報(例えば、前述の第三者機関から取得)と暗号鍵を生成すると共に、その暗号鍵を用いてユーザデータを暗号化し、これらのデータ(ID情報、暗号鍵および暗号化データ)をCD-Rライター52に転送する。CD-Rライター52はパーソナルコンピュータ51から転送されたID情報と暗号鍵をCD-R 53のシステム領域に書き込むと共に、暗号化データをCD-R 53のユーザエリア(UA)に書き込み、以上一連の「ユーザによるデータ書き込み処理」を終了する。

【0062】したがって、この「ユーザによるデータ書き込み処理」によれば、所定のサポートリストに記載された製造者情報をもつCD-Rについてののみ、そのシステム領域にID情報と暗号鍵を書き込むことができると共に、そのユーザエリアに当該暗号鍵で暗号化したユーザデータを書き込むことができる一方、ノーブランド品等の他のCD-Rについては、平文のデータ書き込みを行うことができる。

【0063】その結果、セキュリティ性を希望するユーザは、積極的にサポートディスク(サポートリストに記載された製造者情報をもつCD-R)を使用することとなり、結局、粗悪品の存在を否定できないノーブランドCD-Rの使用を事実上禁止して、CD-Rのデータ書き込みの信頼性確保を図ることができる。

【0064】<ユーザによるデータ再生処理>図10は、ユーザ段階で実行されるデータ再生動作(以下「ユーザによるデータ再生処理」という。)を示すフローチャートである。この処理では、ユーザは、前述のユーザによるデータ書き込み処理によって、ID情報および暗号鍵ならびに暗号化データが書き込まれたCD-R 1を入手し、そのCD-R 1をCD-R記録再生装置30にセットして、そのCD-R 1から暗号鍵と暗号化データを読み出し、暗号鍵を用いて暗号化データを復号するという一連の処理を実行する。この一連の処理において、とりわけ重要な点は、二種類のユーザが存在することにある。第一のユーザは正当なID情報を知っているユーザ(以下「正規ユーザ」という。)であり、第二のユーザは正当なID情報を知らないユーザ(以下「不正ユーザ」という。)である。

【0065】図10において、ユーザによるデータ再生処理を開始すると、CD-R記録再生装置30は、ホスト装置41からの再生命令の有無を判定する(ステップS41)。そして、再生命令があると、ホスト装置41に対してID入力要求を発行し(ステップS42)、ホ

スト装置41は、画面上にID入力を促す旨の所定のGUI(Graphical User Interface)を表示してユーザによるキーボード等からのID入力を受け付け(ステップS43)、入力されたID情報をCD-R記録再生装置30に転送する。

【0066】CD-R記録再生装置30は、CD-R 1のシステム領域に書き込まれているID情報を読み出して、ホスト装置41から転送されたID情報との一致を判定し(ステップS44)、不一致であれば不正ユーザと判断してそのまま処理を終了する一方、一致であれば正規ユーザと判断して、CD-R 1のシステム領域に書き込まれている暗号鍵とデータエリアに書き込まれている暗号化データとを読み出してホスト装置41に転送する(ステップS45)。ホスト装置41は、その暗号鍵を用いて暗号化データを復号し、当該復号データに対する正規ユーザのアクセスを許容した後、処理を終了する。

【0067】図11は、上記「ユーザによるデータ再生処理」のタイムランを示す図であり、図中のパーソナルコンピュータ51は上述のホスト装置41に相当するもの、CD-Rライター52は上述のCD-R記録再生装置30に相当するもの、CD-R 53は上述のCD-R 1に相当するものである。

【0068】この図において、ユーザは、CD-R 53をCD-Rライター52に装填すると共に、パーソナルコンピュータ51を操作して所要の再生命令をCD-Rライター52に発行する。CD-Rライター52はこの再生命令に応答してID要求をパーソナルコンピュータ51に返し、パーソナルコンピュータ51は画面上にID入力を促す旨のGUIを表示する。ユーザは、そのGUIに従って所定のID情報(CD-R 53の配布先から正当に通知されたID情報)を入力し、パーソナルコンピュータ51は入力されたID情報をCD-Rライター52に転送する。

【0069】CD-Rライター52は、CD-R 53のシステム領域に書き込まれているID情報を読み出し、パーソナルコンピュータ51から転送されたID情報との一致を判定して、不一致であれば不正ユーザと判断し、処理を中止して再生を拒否する一方、一致していれば正規ユーザと判断し、CD-R 53のシステム領域に書き込まれている暗号鍵とデータエリアに書き込まれている暗号化データとを読み出してパーソナルコンピュータ51に転送する。パーソナルコンピュータ51は、その暗号鍵を用いて暗号化データを復号し、正規ユーザからのアクセスを許容した後、以上一連の「ユーザによるデータ再生処理」を終了する。

【0070】したがって、この「ユーザによるデータ再生処理」によれば、CD-Rのシステム領域に書き込まれているID情報を用いて正規ユーザと不正ユーザとを識別することができると共に、正規ユーザによってデー

タ再生処理が行われている場合に限り、CD-Rのシステム領域に書き込まれた暗号鍵とデータエリアに書き込まれた暗号化データとをホスト装置に転送し、ホスト装置で暗号化データの復号を行い、復号された生データへのアクセス（例えば、データの閲覧ないし実行等）を許可することができる。

【0071】その結果、不正ユーザを排除してデータの再生を行うことができ、データの不正閲覧および不正実行等を防止し、以って、CD-Rのセキュリティ性を向上することができる。

【0072】＜ユーザによるディスクコピー処理＞図12は、ユーザ段階で実行されるディスクコピー動作（以下「ユーザによるディスクコピー処理」という。）を示すフローチャートである。この処理では、ユーザは、前述のユーザによるデータ書き込み処理によって、ID情報および暗号鍵ならびに暗号化データが書き込まれたCD-R1を入手し、そのCD-R1をCD-R記録再生装置30にセットして、そのCD-R1から暗号鍵と暗号化データを読み出し、当該暗号鍵を用いて暗号化データを復号し、その復号データを別のCD-R記録再生装置30にセットされた未使用のCD-Rに書き込む（コピーする）という一連の処理を実行する。この一連の処理においても、正当なID情報を知っている正規ユーザと正当なID情報を知らない不正ユーザの二種類のユーザが存在する。

【0073】図12において、ユーザによるディスクコピー処理を開始すると、コピー元のCD-R1を装填したCD-R記録再生装置（以下「コピー元CD-R記録再生装置」という。）10は、ホスト装置41からのコピー命令の有無を判定する（ステップS51）。そして、コピー命令があると、ホスト装置41に対してID入力要求を発行し（ステップS52）、ホスト装置41は、画面上にID入力を促がす旨の所定のGUIを表示してユーザによるキーボード等からのID入力を受け付け（ステップS53）、入力されたID情報をコピー元CD-R記録再生装置30に転送する。

【0074】コピー元CD-R記録再生装置30は、CD-R1のシステム領域に書き込まれているID情報を読み出して、ホスト装置41から転送されたID情報との一致を判定し（ステップS54）、不一致であれば不正ユーザと判断してCD-R1のデータエリアに書き込まれた暗号化データを読み出してホスト装置41に転送（ステップS55）する一方、一致であれば正規ユーザと判断してCD-R1のシステム領域に書き込まれているID情報と暗号鍵およびデータエリアに書き込まれている暗号化データを読み出してホスト装置41に転送する（ステップS56）

【0075】ホスト装置41は、その転送データにID情報と暗号鍵が含まれているか否かを判定し、ID情報と暗号鍵が含まれていればそのID情報と暗号鍵および

暗号化データを順次にコピー先のCD-R記録再生装置30（以下「コピー先CD-R記録再生装置」という。）10に転送し、または、ID情報と暗号鍵が含まれていなければ転送データ（暗号化データ）それ自体をコピー先CD-R記録再生装置30に転送する。

【0076】コピー先CD-R記録再生装置30は、転送されたデータにID情報と鍵情報が含まれている場合、前述の「ユーザによるデータ書き込み処理」（図8参照）と同様の手順で、そのID情報と鍵情報をコピー先のCD-Rに記録した後、暗号化データをコピー先のCD-Rのデータエリアに記録し、または、転送されたデータにID情報と鍵情報が含まれていない場合は、暗号化データをコピー先のCD-Rのデータエリアに記録した後、記録完了をホスト装置41に通知して一連のディスクコピー処理を終了する。

【0077】図13は、上記「ユーザによるディスクコピー処理」のタイムランを示す図であり、図中のパーソナルコンピュータ51は上述のホスト装置41に相当するもの、左側のCD-R53aはコピー元のCD-R1に相当するもの、左側のCD-Rライター52aは上述のコピー元CD-R記録再生装置30に相当するもの、右側のCD-Rライター52bは上述のコピー先CD-R記録再生装置30に相当するもの、右側のCD-R53bはコピー先のCD-Rに相当するものである。すなわち、この例では、左側のCD-R53aの記録情報を右側のCD-R53bにディスクコピーする例を示している。

【0078】この図において、ユーザは、コピー元とコピー先のCD-R53a、53bをそれぞれCD-Rライター52a、52bに装填すると共に、パーソナルコンピュータ51を操作して所要のコピー命令をコピー元CD-Rライター52aに発行する。コピー元CD-Rライター52aはこのコピー命令に回答してID要求をパーソナルコンピュータ51に返し、パーソナルコンピュータ51は画面上にID入力を促がす旨のGUIを表示する。ユーザは、そのGUIに従って所定のID情報（CD-R53aの配布先から正当に通知されたID情報）を入力し、パーソナルコンピュータ51は入力されたID情報をコピー元CD-Rライター52aに転送する。

【0079】コピー元CD-Rライター52aは、CD-R53aのシステム領域に書き込まれているID情報を読み出し、パーソナルコンピュータ51から転送されたID情報との一致を判定して、不一致であれば不正ユーザと判断し、暗号化データのみの限定的コピーを許可する一方、一致していれば正規ユーザと判断し、CD-R53aのシステム領域に書き込まれているID情報と暗号鍵およびデータエリアに書き込まれている暗号化データを読み出してパーソナルコンピュータ51に転送する

【0080】パーソナルコンピュータ51は、コピー先CD-Rライター52bに書き込み命令を発行すると共に、コピー元のCD-R53aから読み出したID情報、暗号鍵および暗号化データをコピー先CD-Rライター52bに転送する。コピー先CD-Rライター52bはそのID情報と暗号鍵をCD-R53bのシステム領域に書き込むと共に、その暗号化データをCD-R53bのデータエリアに書き込み、その書き込み完了をホスト装置41に通知して、以上一連の「ユーザによるディスクコピー処理」を終了する。

【0081】したがって、この「ユーザによるディスクコピー処理」によれば、コピー元CD-Rのシステム領域に書き込まれているID情報を用いて正規ユーザと不正ユーザとを識別することができると共に、正規ユーザによってディスクコピー処理が行われている場合に限り、コピー元CD-Rのシステム領域に書き込まれたID情報と暗号鍵およびデータエリアに書き込まれた暗号化データをホスト装置に転送し、ホスト装置からコピー先CD-Rライターに転送して、コピー先CD-Rに書き込む（コピーする）ことができる。

【0082】その結果、正規ユーザだけにディスクコピーを許可してコピー元CD-Rの完全複製物を製造させることができる一方、不正ユーザに対しては暗号化データのみの限定的コピーを許可し、実質的に再利用不能（暗号を解読しない限りデータを利用できない）な未完成複製物を製造させることができ、海賊版CD等の不正複製物の出現を防止して、CD-Rのセキュリティ性の向上を図ることができる。

【0083】＜まとめ＞以上、説明したとおり、本実施の形態のCD-R1は、サポートリストに記載された製造者のCD-R1を使用して記録データの書き込みを行う場合に限り、その記録データを暗号化して書き込む一方、サポートリストに記載されていない製造者（または製造者不明）のCD-Rを使用して記録データの書き込みを行う場合は当該記録データを平文で書き込むようにしたから、秘匿を要するデータの保管や配布を行おうとするユーザは、当然のことながら積極的に上記サポートリストに記載された製造者のCD-R1を使用することとなり、その結果、ノーブランド品の使用を阻止して粗悪品に起因する書き込みや読み出しのトラブルを回避することができるという格別有益な効果が得られる。

【0084】また、CD-R1のシステム領域に、暗号鍵と共にID情報を書き込むため、このID情報を用いて、事後のデータ再生やデータコピーの際のユーザ認証を行うことができ、正規ユーザに対してのみデータ再生やデータコピーを許容することができるうえ、万が一不正にコピーされた場合でも、そのID情報から追跡調査を行うことができる。

【0085】また、かかるメリットを奏するためには製造時に、CD-R1のディスク情報に製造者を特定可能

な情報を含めるとともに、上記のサポートリストに製造者の情報を登録するだけでよく、しかも、ATIP情報のリードイン開始位置情報などの既存情報を製造者の特定情報に利用できるから、新たな工程を追加する必要もないという製造上のメリットもある。

【0086】なお、以上の説明では、ID情報や暗号鍵などの隠し情報をシステム領域に書き込んでいるが、このシステム領域とは、ユーザによる直接的なアクセスが許容された領域（典型的にはデータエリア）以外の領域という意味であり、前述のPCAやPMAはもちろんのこと、リードインであってもよいし、リードアウトであってもよく、あるいは、これ以外の領域が存在するならば、その領域であってもよい。

【0087】また、暗号鍵については、特に説明を加えなかったが、一般的に知られている様々な暗号化方式（例えば、前述のDES方式以外にも、FEAL:Fast Encipherment Algorithmなどの方式がある。）のいずれを採用してもかまわない。解読の困難性、暗号化処理や復号処理のオーバーヘッドおよび暗号化データのボリューム等を勘案して適切な方式を採用すればよい。

【0088】また、前記説明のID情報や暗号鍵を利用したセキュリティ機能は、もっぱらCD-R記録再生装置30のコントローラ40やホスト装置41のメインボードに実装されたマイクロコンピュータならびに各種周辺機器を含むハードウェア資産と、オペレーティングシステムや各種プログラム（ドライバソフトを含む）などのソフトウェア資産との有機的結合によって機能的に実現されるものであるが、ハードウェア資産およびオペレーティングシステムは汎用のものを利用できるから、前記説明のID情報や暗号鍵を利用したセキュリティ機能にとって欠くことのできない必須の事項は、実質的に、前述の「ユーザによるデータ書き込み処理」（図8参照）、「ユーザによるデータ再生処理」（図10参照）または「ユーザによるディスクコピー処理」（図12参照）などのプログラムに集約されているということがいえる。

【0089】したがって、本発明に係るID情報や暗号鍵を利用したセキュリティ機能は、それらのプログラムのすべてまたはその要部を格納した、フロッピーディスク、光ディスク、コンパクトディスク、磁気テープ、ハードディスクまたは半導体メモリなどの記録媒体若しくはこれらの記録媒体を含む構成部品（ユニット品や完成品または半完成品）を包含する。なお、その記録媒体または構成部品は、それ自体が流通経路にのるものはもちろんのこと、ネットワーク上にあって記録内容だけを提供するものも含まれる。

【0090】また、以上の説明では、ライトワンス型光ディスクとしてCD-Rの例を示したが、これに限らない。例えば、DVD（Digital Video DiscまたはDigital Versatile Disc）-Rも1回だけのデータ書き込みを

行うことができるから、もちろんライトワンス型光ディスクの仲間である。上記説明をDVD-Rに適用する場合、CD-RをDVD-Rと読み替えると共に、CD-R記録再生装置やCD-RライターをそれぞれDVD-R記録再生装置、DVD-Rライターと読み替ればよい。

#### 【0091】

【発明の効果】請求項1記載の発明によれば、所定の製造者によって作られたライトワンス型光ディスクについてのみ、そのシステム領域の一部にセキュリティ対策のための情報が書き込まれる。したがって、特に秘匿を要するデータの保管や配布を行う際に、当該所定の製造者によって作られたライトワンス型光ディスクの使用を強制することができる。

【0092】請求項2記載の発明によれば、データの再生時にその存在が無視される特定の領域（レーザ強度キャリブレーション用領域）にセキュリティ対策のための情報が書き込まれるため、当該領域はユーザに対して不可視であるばかりか、当業者にとってもレーザ強度キャリブレーション用として広く理解されているため、かかる専門知識を有する当業者に対しても不可視性を確保でき、セキュリティを保つことができる。

【0093】請求項3記載の発明によれば、いずれもユーザからの直接的なアクセスが許容されていない領域にセキュリティ対策のための情報が書き込まれるため、当該情報をユーザからの隠し情報とすることができる。

【0094】請求項4記載の発明によれば、ライトワンス型光ディスクの固体識別に基づくセキュリティ対策が可能となり、不正コピー等を防止し、データ再生時のセキュリティを向上することができる。

【0095】請求項5記載の発明によれば、セキュリティ対策のための情報を利用したユーザ認証が可能となり、その認証結果を用いて不正ユーザを排除し、データ再生時のセキュリティを向上することができる。

【0096】請求項6記載の発明によれば、セキュリティ対策のための情報を利用したユーザデータの暗号化が可能となり、万が一不正認証された場合でも、生データが露呈しないため、データの秘匿性を確保することができる。

【0097】請求項7記載の発明によれば、セキュリティ対策のための情報を利用した暗号化データの復号が可能となり、万が一不正認証された場合でも、セキュリティ対策のための情報が読み取られない限り、生データが露呈せず、データの秘匿性を確保することができる。

【0098】請求項8記載の発明によれば、所定の製造者によって作られたライトワンス型光ディスクについてのみ、そのシステム領域にセキュリティ対策のための情報が書き込まれる。したがって、特に秘匿を要するデータの保管や配布を行う際に、当該所定の製造者によって作られたライトワンス型光ディスクの使用を強制するこ

とができる。

【0099】請求項9記載の発明によれば、マイクロコンピュータを含むハードウェア資産と該プログラムとの有機的結合によって前記アクセス手段、読み出し手段、判定手段および書き込み手段を実現することができる。

#### 【図面の簡単な説明】

【図1】ライトワンス型光ディスクの外観図およびその要部拡大図である。

【図2】CD-Rの断面構造図である。

【図3】CD-Rに形成される案内溝（ウォッブルグループ）を示す模式図である。

【図4】CD-Rに案内溝を形成するために主としてディスクの製造段階で用いられる製造装置の構成図である。

【図5】CD-Rの各記録領域のフォーマット概念図である。

【図6】製造時にシステム領域に書き込まれるID情報と暗号鍵を含むデータフォーマットの例示構造図である。

【図7】ライトワンス型光ディスク記録再生装置の概略的なブロック構成図である。

【図8】ユーザ段階で実行されるデータ書き込み動作（ユーザによるデータ書き込み処理）を示すフローチャートである。

【図9】ユーザによるデータ書き込み処理のタイムランを示す図である。

【図10】ユーザ段階で実行されるデータ再生動作（ユーザによるデータ再生処理）を示すフローチャートである。

【図11】ユーザによるデータ再生処理のタイムランを示す図である。

【図12】ユーザ段階で実行されるディスクコピー動作（ユーザによるディスクコピー処理）を示すフローチャートである。

【図13】ユーザによるディスクコピー処理のタイムランを示す図である。

#### 【符号の説明】

PCA Power Calibration Area（システム領域、レーザ強度キャリブレーション用領域）

PMA Program Memory Area（システム領域、セッション情報の一時格納用領域）

R1 リードイン（セッション情報格納用領域）

RO リードアウト（ユーザ領域の終了位置を明示するための領域）

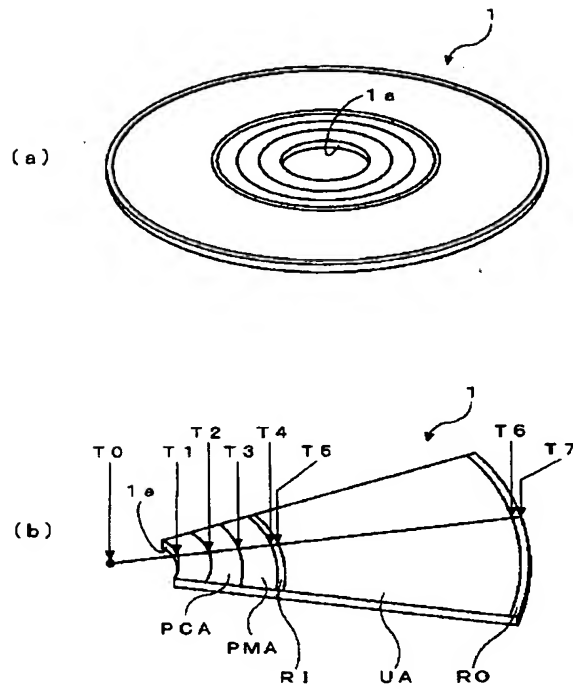
UA ユーザエリア（ユーザ領域）

1 CD-R（ライトワンス型光ディスク）

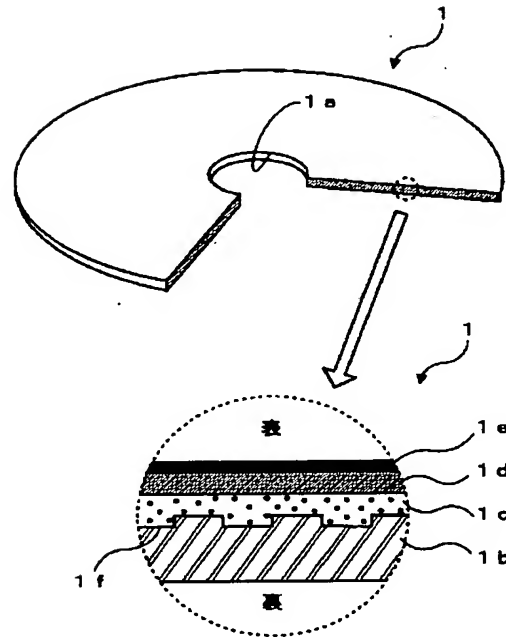
10 CD-R記録再生装置（ライトワンス型光ディスク用記録装置）

20 コントローラ（アクセス手段、読み出し手段、判定手段、書き込み手段）

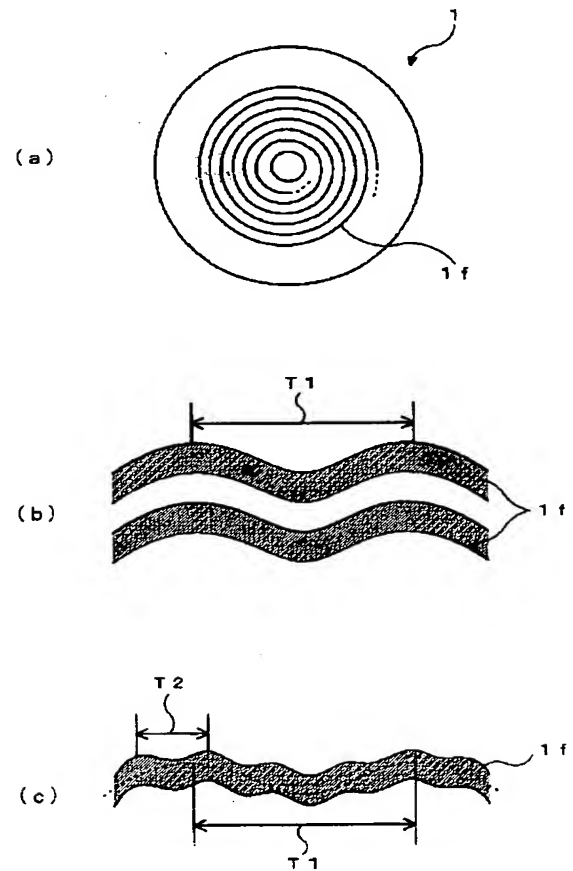
【図1】



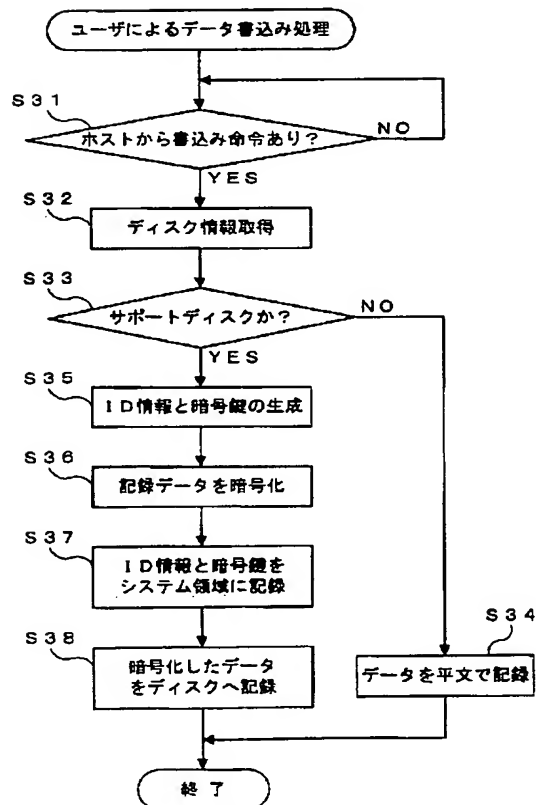
【図2】



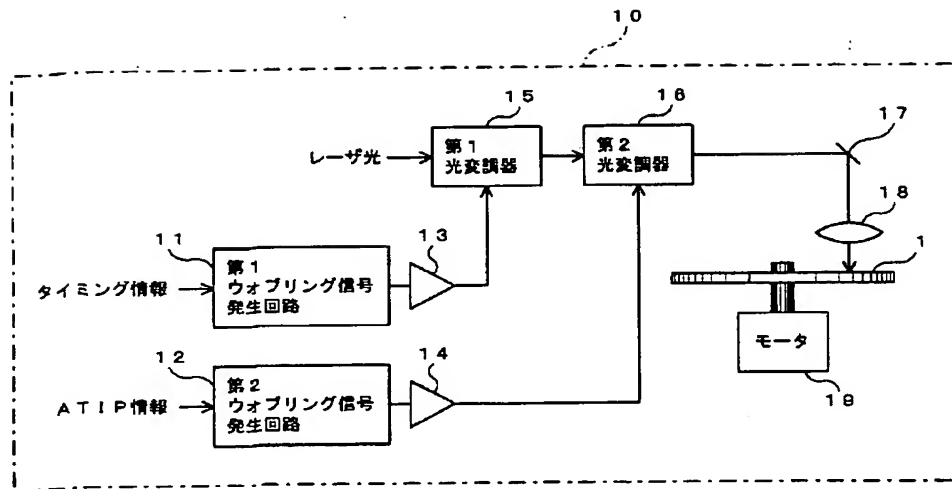
【図3】



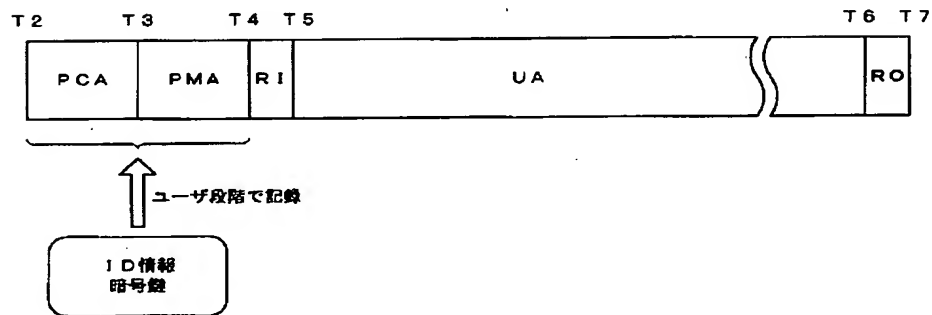
【図8】



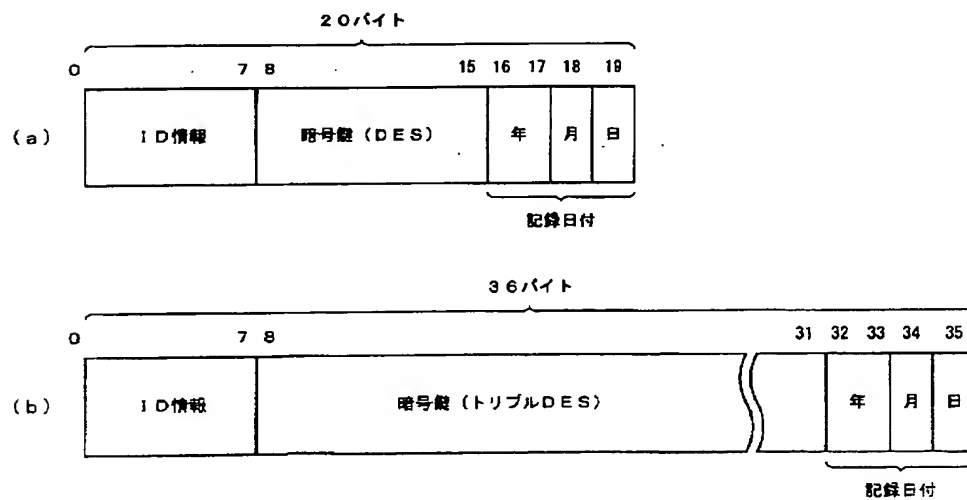
【図4】



【図5】

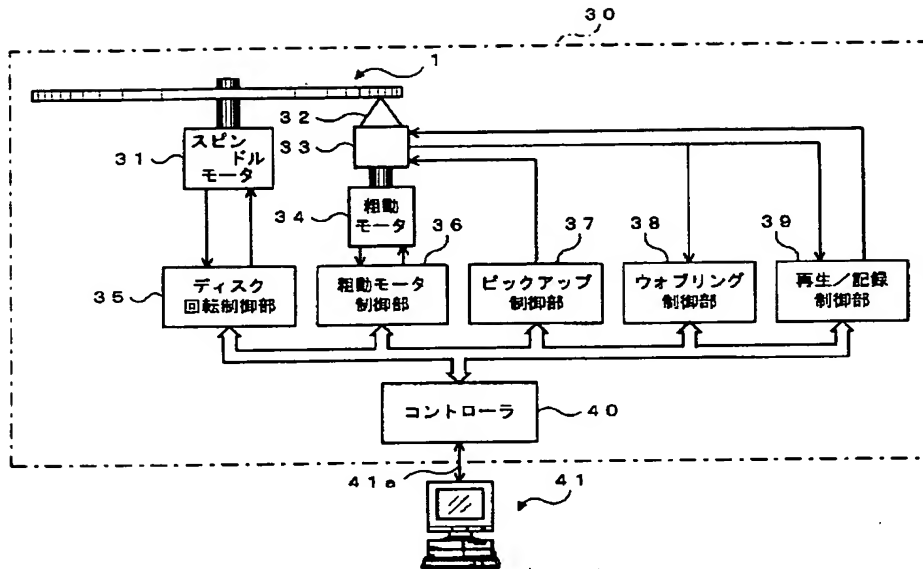


【図6】

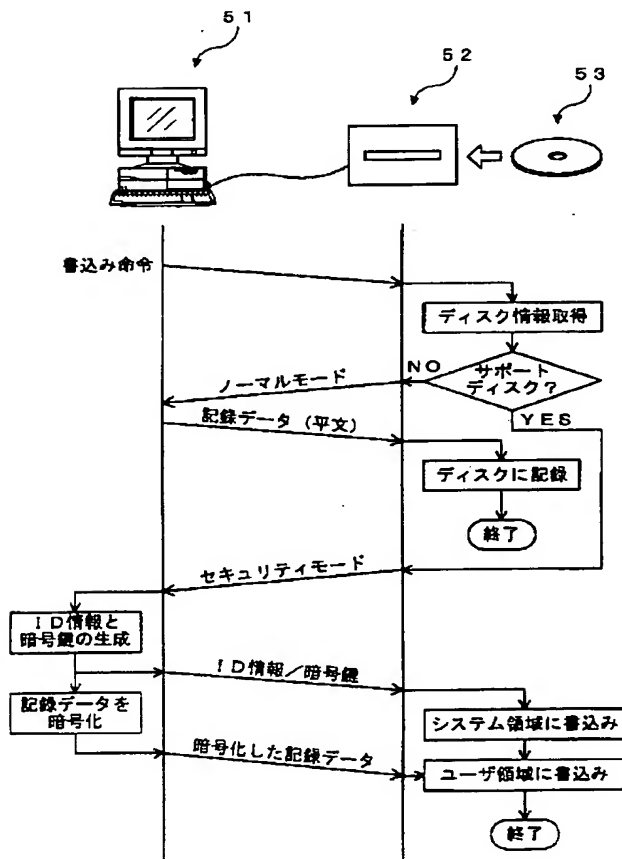




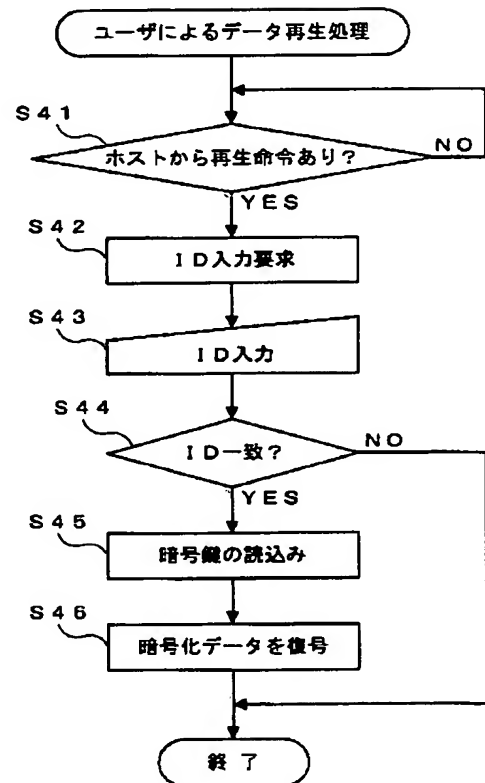
【図 7】



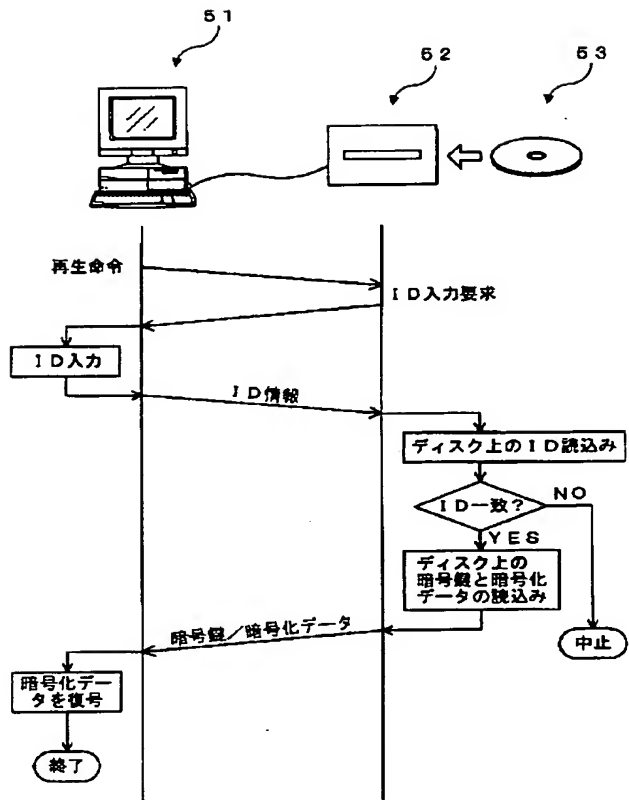
【図 9】



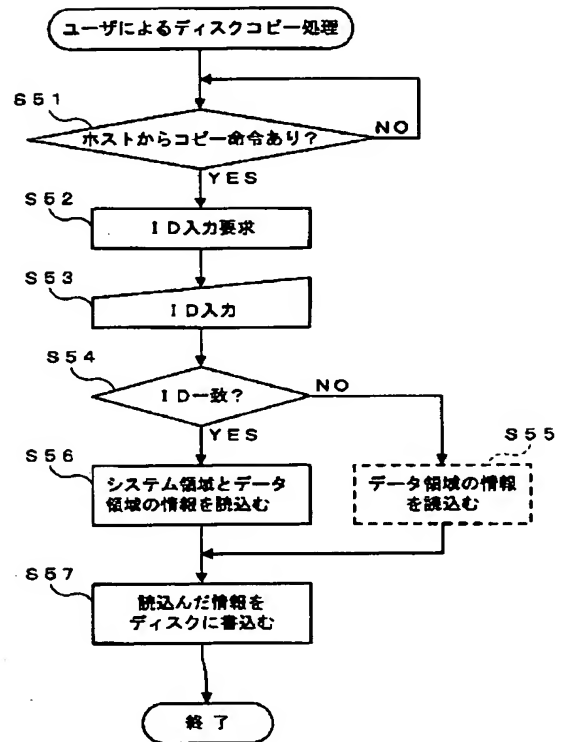
【図 10】



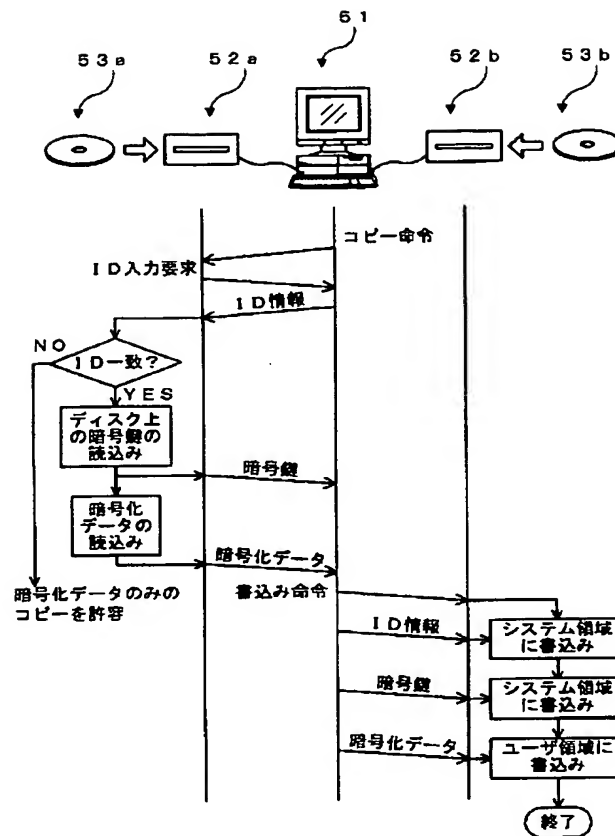
【図11】



【図12】



【図 13】



フロントページの続き

(72) 発明者 清水 洋信  
 東京都台東区上野 6 丁目 16 番 20 号 太陽誘  
 電株式会社内

F ターム (参考) 5D044 AB01 AB05 AB07 BC05 CC04  
 DE49 DE50  
 5D066 DA12  
 5D090 AA01 BB03 CC14 DD02 DD05  
 FF24 GG32